CLAIMS

1. A secret key registration method for registering a secret key of each entity for use in cryptographic communication, comprising the steps of:

at each entity, generating a plurality of passwords based on a basic password;

sending the generated passwords to a plurality of key registration agencies, respectively; and

at each entity, receiving its secret keys which have been encrypted based on the respective passwords from the key registration agencies, respectively.

2. The secret key registration method as set forth in claim 1, wherein

the passwords are generated at each entity based on the basic password and a plurality of different one-way functions.

3. the secret key registration method as set forth in claim 2, wherein

each of the one-way functions is a one-way hash function.

4. The secret key registration method as set forth in claim 1, wherein

at each entity, the respective passwords are encrypted according to a public key method and the encrypted passwords are sent to the key registration agencies, respectively.

5. A secret key register for registering a secret key of each entity for use in cryptographic communication, comprising

a controller capable of performing the following operations:

(i) generating a plurality of passwords based on a basic password;

(ii) sending the generated passwords to a plurality of key registration agencies, respectively; and

(iii) receiving secret keys of each entity which have been encrypted based on the respective passwords from the key registration agencies, respectively.

6. The secret key register as set forth in claim 5 wherein

the passwords are generated based on the basic password and a plurality of different one-way functions.

7. The secret key register as set forth in claim 6, wherein

each of the one-way functions is a one-way hash function.

8. The secret key register as set forth in claim 5, wherein

the respective passwords are encrypted according to a public key method and the encrypted passwords are sent to the key registration agencies, respectively.

9. A secret key issuing method for issuing a secret key of each entity for use in cryptographic communication by each of a plurality of key issuing agencies, comprising the steps of:

at each entity, generating a plurality of passwords based on a basic password;

sending the generated passwords to the key issuing agencies, respectively; and

at the key issuing agencies, issuing secret keys of each entity which have been encrypted based on the respective passwords, respectively.

10. The secret key issuing method as set forth in claim 9, wherein

the passwords are generated at each entity based on the basic password and a plurality of different one-way

functions.

11. The secret key issuing method as set forth in claim 10, wherein

each of the one-way functions is a one-way hash function.

12. The secret key issuing method as set forth in claim 9, wherein

at each entity, the respective passwords are encrypted according to a public key method and the encrypted passwords are sent to the key issuing agencies, respectively.

13. The secret key issuing method as set forth in claim 9, wherein

at each entity, the respective passwords and its electronic mail address are sent to the respective key issuing agencies via a homepage on the Internet, and at each key issuing agency, a secret key of each entity is issued by means of electronic mail.

14. The secret key issuing method as set forth in claim 9, wherein

at each entity, the respective passwords are sent to

the respective key issuing agencies by means of electronic mail, and at each key issuing agency, a secret key of each entity is issued by means of electronic mail.

15. The secret key issuing method as set forth in claim 9, wherein

at each key issuing agency, a secret key of each entity is issued by using divided identification information obtained by dividing identification information of each entity.

16. A cryptographic communication method for transmitting information in ciphertext form between first and second entities, comprising the steps of:

at the first and second entities, generating a plurality of passwords based on a basic password;

sending the generated passwords to a plurality of key issuing agencies, respectively;

at each key issuing agency, generating and sending secret keys of the respective first and second entities which have been encrypted based on the respective passwords;

at the first entity, generating a first common key based on the secret keys of the first entity sent from the respective key issuing agencies and identification information of the second entity as a destination;

at the first entity, encrypting a plaintext into a ciphertext by using the generated first common key and transmitting the ciphertext to the second entity;

at the second entity, generating a second common key identical with the first common key, based on the secret keys of the second entity sent from the respective key issuing agencies and identification information of the first entity as a destination; and

at the second entity, decrypting the transmitted ciphertext into a plaintext by using the generated second common key.

17. The cryptographic communication method as set forth in claim 16, wherein

the passwords are generated at the first and second entities based on the basic password and a plurality of different one-way functions.

18. The cryptographic communication method as set forth in claim 17, wherein

each of the one-way functions is a one-way hash function.

19. The cryptographic communication method as set forth in claim 16, wherein

at the first and second entities, the respective passwords are encrypted according to a public key method and the encrypted passwords are sent to the respective key issuing agencies.

20. A cryptographic communication system for performing an encryption process of encrypting a plaintext as information to be transmitted into a ciphertext and a decryption process of decrypting the transmitted ciphertext into a plaintext mutually between a plurality of entities, comprising:

a plurality of entities for respectively generating a plurality of passwords based on a basic password and sending the generated passwords to a plurality of key issuing agencies; and

a plurality of key issuing agencies for respectively issuing secret keys of each entity which have been encrypted based on the respective passwords.

21. The cryptographic communication system as set forth in claim 20, wherein

each of the entities generates the passwords based on the basic password and a plurality of different one-way functions.

22. The cryptographic communication system as set forth in claim 21, wherein

each of the one-way functions is a one-way hash function.

23. The cryptographic communication system as set forth in claim 20, wherein

each of the entities encrypts the respective passwords according to a public key method and sends the encrypted passwords to the respective key issuing agencies.

24. A computer memory product having computer readable program code means for causing a computer to register a secret key of each entity for use in cryptographic communication, said computer readable program code means comprising:

program code means for causing the computer to generate a plurality of passwords based on a basic password;

program code means for causing the computer to send the generated passwords to a plurality of key registration agencies, respectively; and

program code means for causing the computer to receive secret keys of each entity which have been encrypted based on the respective passwords from the key

registration agencies, respectively.

25. The computer memory product as set forth in claim 24, wherein

the passwords are generated on the basic password and a plurality of different one-way functions.

26. A computer data signal embodied in a carrier wave for transmitting a program, the program being configured to cause a computer to register a secret key of each entity for use in cryptographic communication, comprising:

a code segment for causing the computer to generate a plurality of passwords based on a basic password;

a code segment for causing the computer to send the generated passwords to a plurality of key registration agencies, respectively; and

a code segment for causing the computer to receive secret keys of each entity which have been encrypted based on the respective passwords from the key registration agencies, respectively.

27. The computer data signal embodied in a carrier wave as set forth in claim 26, wherein

the passwords are generated on the basic password

and a plurality of different one-way functions.